Organized Crime and the Internet: Implications for National Security

Peter Grabosky

Australian National University

Introduction

The extent to which organized criminal use of the Internet poses a threat to national or international security depends upon two basic definitional issues: 1) What is security? and 2) What is organized crime? This essay addresses these issues, and then proceeds to a discussion of situations in which security has been threatened, or is likely to be, by organized cybercriminal activity. The increasing pervasiveness of digital technology makes its continuing exploitation for criminal purposes inevitable. Some of these may threaten security, but others not.

What is security?

The concept of national security has been broadened in recent years. Traditionally, it was limited to a state's capacity to defend its territorial borders against the invading armed forces of rival nation states. Later, it was extended to embrace state capacity to provide for the basic well-being of its citizens.[1] More recently, it has been expanded further to embrace such broader considerations as human security, with its greater focus on groups and individuals.[2] However, this more expansive notion is hardly new. Consider the following observation, made over two thousand years ago:

> Plans and projects for harming the enemy are not confined to any one method. Sometimes entice his wise and virtuous men away so that he has no counsellors. Or send treacherous people to his country to wreck his administration. Sometimes use cunning deceptions to alienate his ministers from the sovereign. Or send skilled craftsmen to encourage his people to exhaust their wealth. Or present him with licentious musicians and dancers to change his customs. Or give him beautiful women to bewilder him.[3]

If indeed military strength remains the foundation of security today, it in turn depends upon other basic factors. These include a strong economy, and a well-educated, healthy, productive and cohesive citizenry. Moreover, the pervasiveness of digital technology has profound security implications. In the developed world at least, critical infrastructure such as power

generation, telecommunications, finance, and defence systems are all supported by, and dependent upon, digital technology. Sun Tzu's broad thinking is as relevant now as it was during his lifetime.

Not all security threats emanate from state action. Some arise from natural causes. Pandemics and extreme weather events can weaken more vulnerable states. Non-state actors, at least those perceived to be enemies of the state, have long been regarded as threats to security, both internal and external. This was reinforced by the events of September 11, 2001. With the end of the Cold War, and the significant increase in recreational drug use in Western nations, the security implications of conventional criminality began receiving greater attention. Transnational crime (most of it organized) was most prominently deemed to be a security threat in President Clinton's address to the United Nations General Assembly in 1995.[4]

There is, of course, an element of ambiguity to the concept of national security. Just as individuals may be paranoid or hypochondriac, so too may leaders and their publics suffer unwarranted anxiety. Things may be perceived as intensely threatening to some, when they are objectively trivial. Predictions of Doomsday are frequently made, but have yet to be realized. Ironically, the sources of some anxiety can prove to be positively beneficial. J. Edgar Hoover, former Director of the FBI, regarded the civil rights movement of the 1960s as a national security threat.[5] The Nixon administration argued that publication of the Pentagon Papers would jeopardise the national security of the United States.[6] More recently a member of the US Congress referred to Wikileaks as presenting "a clear and present danger to the national security of the United States." [7]

Threats to security may be invoked cynically, for ulterior motives. Some leaders raise the spectre of security threat for domestic political purposes. The Nixon White House asserted national security as justification for terminating investigation of the Watergate burglary.[8] As we will see, claims that organized cybercrime threaten national security are not uncommon. Some may in fact be valid, but none should be uncritically accepted at face value. The term "hypersecuritization" applies as much to cyberspace as it does on the Earth's surface.[9]

What is organized crime?

Organized crime lacks a universally accepted meaning. Klaus von Lampe has identified no less than 150 definitions of organized crime.[10] Whatever one's preferred definition, the

conventional conception of organized crime is out of date, having been overtaken by the evolution of the phenomenon itself. The classic "mafia model" that served as the basis of Cressey's[11] analysis of four decades ago conjured up visions of ethnically-based, monolithic, hierarchical organizations ruled by "Mr Bigs." By the 1990s, observers of criminal organizations reported that rather than the work of formal, enduring structures, a significant amount of criminal activity was undertaken by loose coalitions of smaller groups converging temporarily to exchange goods and services.[12] The idea of vertically integrated enterprises thus gave way to the metaphor of networks,[13] which provided a foundation for contemporary thinking about the interrelationships within organized criminal groups and between individual groups.

Developments in organizational and criminal life have evolved rapidly in recent years, leaving some definitions of organized crime too narrow and too constrained by ideology. Traditional definitions of organised crime have tended to be based on the profit motive. However, even the most insightful observers of "terrestrial" organized crime note the intrinsic attraction of excitement, comradeship and other non-material values. As we shall see, a great deal of organized criminal activity on the internet is driven primarily by non-monetary considerations. These include the quest for intellectual challenge, individual or group notoriety, lust (in the case of organized paedophile activity), ideology, rebellion, and curiosity. Today, there are many criminal organizations that do not practice violence or engage in bribery. Moreover, the traditional view of criminal organizations consisting of full or part time professional criminals was also somewhat simplistic. Some criminal organizations have explicit or implicit membership, but may also include a variety of hangers-on, camp followers, and accomplices, some of whom will be well aware of their complicity in criminal enterprise, while others may not.

The boundaries of organized crime are not always clear cut. One of the more interesting manifestations of conceptual convergence concerns the intersection of organized crime and terrorism. Terrorism, too, can be a slippery term. The definition of terrorism employed here is the following: "An act or threat of violence to create fear and/or compliant behavior in a victim or wider audience for the purpose of achieving political ends."[14] The underscored words are important. Organized criminals have been known to engage in acts of terrorism: The assassinations of Italian Judges Giovanni Falcone and Paolo Borsellino were political statements as much as they were Mafia "hits." Much terrorism is undertaken collectively, with varying degrees of organization. Most terrorist acts are, by definition, criminal acts.

There is also a degree of occupational mobility across definitional boundaries. Some criminals become terrorists, and some terrorists give up the political struggle for a life of crime. Some criminal and terrorist organizations collaborate. The terms "crime-terrorism continuum" "fighters turned felons" and "marriages of convenience" are illustrative.[15]

Today, it requires an exceptionally closed mind to deny that *states are also capable of criminal acts*. Throughout recorded history, crimes by state actors have occurred in times of peace, as well as during armed conflicts. Most recently, one notes allegations of drug manufacture and counterfeiting by agents of the Democratic People's Republic of Korea.[16] States have also engaged periodically in kidnapping and assassination, at home and abroad. Today, the business of the International Criminal Court is booming, notwithstanding the refusal of some states to submit to its jurisdiction.

Just as the distinctions between public and private sectors have blurred in recent years with regard to legitimate activities such as public-private partnerships, contracting out, and other mechanisms for the co-production of governance,[17] there is a long tradition of public/private collaboration in criminal activity in furtherance of state interests. Administrators of the French Concession in Shanghai during the 1920s and 1930s relied upon the Green Gang to suppress industrial unrest and regulate drug markets.[18] The US Central Intelligence Agency engaged burglars and criminals around the world to conduct break-ins and kidnappings, and enlisted mafia members in an unsuccessful attempt to assassinate Cuban President Fidel Castro.[19] Toward the end of the Apartheid era, South African state security engaged criminal groups to assist with "sanctions busting" and with resisting ANC insurgents.[20]

Hybrid forms of state-private collaboration may be situated along a continuum, the poles of which represent "purely" private activity on the one hand, and the state itself engaged in organized criminality on the other. Between these polar opposites, one may observe situations where the state turns a blind eye to private criminality; where it implicitly condones criminal activity; where the state actively encourages such activity, but at arm's length; or where it systematically collaborates with its private criminal partners.

Organized cybercrime

By cyber crime, we refer broadly to criminal activity involving information systems as instruments or as targets of illegality. This would entail unlawful access to systems, interference with their lawful use, or theft or destruction of information contained therein. It

may also entail possession or transmission of prohibited content.[21] For present purposes, the fundamental question is whether organized cyber crime has reached the scale and intensity to threaten national security.

Digital technology has empowered individuals as never before. Singlehandedly, teenagers have succeeded in disabling air traffic control systems, shutting down major e-retailers, and manipulating trades on the NASDAQ stock exchange.[22] What individuals can do, organizations can also do, and often better. Just as legitimate organizations have become more efficient and effective through their use of digital technology, so too have criminal organizations. The Internet and related technologies lend themselves perfectly to coordination across a dispersed network. Moreover, the pervasiveness of digital technology has provided tools of crime, and opportunities for crime, that are without precedent.

Organizational forms

The blending of public and private in advanced industrial societies means that the space of cyber criminality is one of great fluidity. On one day, a professional cyber criminal may be working for a government, the next day for himself, and the day after that, for a criminal organization.

The anonymity afforded by the internet makes it relatively easy to conceal one's identity. Skilled hackers, whether employed by the state, by a criminal organization, or working on their own, are often able to avoid attribution. As a result, when one's information systems are subject to intrusion, one cannot be sure whether the intruder is a sole teenager, an organised criminal group, or agents of a foreign government. Indeed, two or more of these may be acting in concert, under arrangements of sponsorship or some hybrid form. Nor can one be confident of the physical location from which the attack originated. It has become a cliché to suggest that cyberspace knows no boundaries, and a crime can be committed against a target on the other side of the world as easily as a target in one's own jurisdiction.

The standard definition of organised crime, based on three or more persons in concert, does not extend to certain highly sophisticated forms of organization such as the mobilization of "botnets" (shorthand for robot network). This involves an offender using malicious software to acquire control over a large number of computers (the largest including more than one million separate machines).[23] Even though the individual and institutional custodians of

compromised computers may be unwitting participants in a criminal enterprise, some commentators maintain that botnets themselves should be considered a form of organised crime.[24]

Criminal use of the Internet

The Internet may be used for criminal activity in three basic ways. It can serve as the **instrument** of crime, the **target** of crime, and it can be used **incidentally** in furtherance of criminal activity. The three modes apply to both individual and organizational use, and are not mutually exclusive. A distinctive characteristic of cybercrime is its "borderless" nature; the offender, the victim, and the evidence of a crime may each be located in different physical locations around the world.

The internet is commonly used as an **instrument** for attacking other computer systems. Most cyber crimes begin when an offender obtains unauthorised access to another system. Systems are often attacked in order to destroy or damage them and the information that they contain. This can serve the purpose of vandalism, protest, or activity in furtherance of other political objectives. One of the more common forms is the "distributed denial of service attack" (DDoS). This entails flooding a target computer system with a massive volume of information so that the system slows down significantly. Botnets are quite useful for such purposes, as are multiple coordinated service requests.

One example of a botnet-initiated DDoS attack occurred in April 2007, when government servers in Estonia were seriously degraded for a number of hours. The attacks appear to have originated in Russia, and are alleged to have resulted from the collaboration of Russian youth organizations and Russian organized crime groups, condoned by the state, although the degree to which the Russian government was complicit in the attacks was unclear.

This raises the question whether certain types of cybercrime may be considered acts of war. Traditionally, an act of war entails threat or use of force by one state against the territorial integrity or political independence of another. This has tended to involve armed invasion or air attack, recently by missiles or by unmanned aerial vehicles or drones. In 2010, it became apparent that the control systems supporting the Iranian Government's nuclear enrichment program had been infected by malicious code, and as a result, a considerable number of fragile centrifuges had been destroyed.[25]

Insurgent and extremist groups have used internet technology as an instrument of theft in order to enhance their resource base. The internet can also be used as a vehicle for fraud. Spurious investment solicitations, marriage proposals, and a variety of other fraudulent overtures are made daily by the hundreds of millions. Imam Samudra, convicted architect of the 2002 Bali bombings, reportedly called upon his followers to commit credit card fraud in order to finance militant activities.[26]

In recent years, the internet has been used to communicate a wide variety of content deemed offensive to the point of criminal prohibition in one or more jurisdictions. Such material includes child pornography, neo Nazi propaganda, or advocacy of Tibetan independence, to specify but a few. Jihadist propaganda and incitement messages also abound in cyberspace.

Digital technology can also be used to obtain, copy and disseminate various forms of intellectual property. So-called information piracy involves appropriation of music, video, and software, and occurs today on a global scale. The software and entertainment industries allege that losses to such thefts have reached billions of dollars.[27]

Information systems may be **targeted** for the data they contain, including banking and credit card details, commercial trade secrets, and classified information held by governments. This too may begin with unauthorised access to a computer system. Theft of personal financial details has provided the basis for thriving markets in such data, which enable fraud on a significant scale.[28]

The quest for state secrets is not limited to officials of rival states. Political espionage has often relied upon the engagement of private individuals to do some of the government's "dirty work." One of the earliest examples of cyber espionage involved a group of East German hackers who obtained access to computer systems at US defence installations on behalf of the KGB.[29] More recently, private organizations have sought to obtain and to disseminate classified information as a matter of principle, specifically, the principle of freedom of information. Most prominent of these is Wikileaks.[30]

Incidental use: As digital technology pervades modern society, we become increasingly dependent upon it to make our lives easier. Much of our ordinary communications and record keeping rely on the internet and related technologies. Just as digital technology enhances the efficiency of our ordinary legitimate activities, so too does it enhance the efficiency of criminal activities. Criminals use the Internet as a medium of communication in furtherance

of criminal conspiracies, or as a means of storing records or other information. Manufacturers of illicit drugs trade recipes over the Internet.[31] The Internet is a convenient medium of communications for terrorists, as it is for law abiding individuals. Jihadi materials are reported to have been stored on the servers of the Arkansas Department of Highways and Transportation.[32] The lengths to which some states will go in order to access online conversations between alleged terrorists (and incidentally, ordinary citizens) is quite substantial. The dramatic growth of the US National Security Agency is indicative.[33] These efforts were not lost on Osama Bin Laden, who reportedly relied on couriers using Internet cafes as a means of communicating with his followers around the world.

Organized cybercrime as a national security threat

Digital technology has become pervasive, and vulnerability to cybercrime has increased commensurately. Nearly two decades have passed since one commentator observed that "everything depends on software."[34] We have already noted that critical infrastructure is now dependent upon digital technology. If one looks at some of the forms that cybercrime has taken in recent years, one can easily recognise the potential risk they pose to national security. The disruption of electronic commerce and banking facilities would threaten one of the major platforms of economic development in the new millennium. One of the most significant developments of modern times is the extent to which digital technology has empowered ordinary people, even teenagers acting alone.[35] Technologies of empowerment also benefit organizations. Anything an individual can do is also within the capacity of organizations, and then some.

Military applications of internet technologies have been openly discussed since at least 1998.[36] Since then, the militarization of cyberspace has continued apace. An unknown number of nations are developing offensive cyber warfare capabilities, which can, inter alia, entail interference with command, control and communications, and disruption or destruction of critical infrastructure. In October, 2012, US Secretary of Defence Leon Panetta spoke of a "cyber-Pearl Harbor" at the hands of a hostile state or extremist group.[37] States too engage in cyber-espionage. It was recently estimated that over 100 countries around the world engage in some form of this activity.[38]

The vulnerability of governmental secrets to theft (notwithstanding the tendency of some keepers of these secrets to overstate their value) was most vividly illustrated by the publication of some 400,000 US State Department diplomatic cables by the organization

Wikileaks.[39] It is unlikely that the duplication and widespread dissemination of such a huge body of information could have occurred without digital technology. Some would argue that the disclosure of classified information is ipso facto a threat to national security; others might contend that the act of classifying information is inherently subjective, and that transparency should take precedence.

The following sections will provide a brief descriptive overview of specific cybercriminal activity attributed to organizations, including observations on the national security implications of each. The selected examples are not intended to be representative of the universe of organized cybercrime, but rather to be illustrative of the great diversity of organized criminal activity reliant on the internet, of their security repercussions, and of the motives of those who commit them.

W0nderland was a members-only group that exchanged illicit images of children, until its interdiction by a multi-national police investigation named Operation Cathedral on September 2, 1998. Simultaneous raids in 14 countries revealed a group of 180 individuals from 49 countries around the world who collectively possessed over 750,000 illicit images of children and over 1,800 digitized videos depicting child abuse. The group had been established in the mid-1990s to facilitate file sharing of the images and videos.[40]

Anonymous is a loose collective of anarchists based largely on a shared ethos of mischief and resentment of authority, who engage in what Professor Dorothy Denning referred to as 'hactivism.'[41] The prevailing ethos of iconoclasm, if not nihilism, began to focus on prominent symbols. The chosen methods were website defacements and distributed denial of service attacks, complemented by online verbal abuse. Not surprisingly, the website of the U.S. Central Intelligence Agency represented an attractive target. Imbued with the hacker ethos that information should be free, the group also targeted the secrecy of the Church of Scientology, the proprietary commercialism of the Motion Picture Association of America, and became a supporter of *Wikileaks*. When the U.S. Government prevailed upon various electronic payment service providers to discontinue processing of contributions to *Wikileaks* after its publication of secret US State Department messages, *Anonymous* orchestrated denial of service attacks against the complying sites.[42]

"Drink or Die" was an international group of copyright pirates who illegally reproduced and distributed software, games and movies over the Internet. They were motivated less by profit than by their desire for recognition as the first group to distribute a perfect copy of a newly

pirated product**.** Founded in Moscow in 1993, the group expanded internationally within three years, with members in more than 12 countries including Britain, Australia, Finland, Norway, Sweden, and the United States. Its approximately 65 members were technologically sophisticated, and included IT professionals skilled in security, programming and internet communications.[43]

The ZeuS virus. Software engineers in Eastern Europe had refined malware known as the ZeuS virus. This malicious code was used by Ukranian hackers to gain access to the computers of individuals employed in variety of small businesses, municipalities, and non-government organizations in the United States. Target computers were compromised when the victim opened an apparently benign email message. With access to the victim's bank account numbers and password details, principals in the Ukraine were able to log on to the target organizations' bank accounts. Accomplices of the Ukranian principals placed notices on Russian language websites inviting students resident in the United States to assist in transferring funds out of the country. These so-called "mules" were provided with counterfeit passports, and were directed to open accounts in false names in various U.S. financial institutions. When principals in the Ukraine transferred funds from legitimate account holders to the mules' accounts, the mules were instructed to move the funds to accounts offshore, or in some cases, to smuggle the funds physically out of the United States. [44]

Dark Market was a forum for the exchange of credit card and banking details, malicious software, and related technology. Its website provided the infrastructure for an electronic bazaar, a meeting place for buyers and sellers of the illicit material. The forum was founded in May, 2005 in order to take advantage of the criminal opportunities presented by the advent of electronic banking and the increasing use of credit and debit cards. Banking and card details were illicitly obtained by various means, including surreptitious recording with 'skimming' devices, unauthorized access to personal or business information systems, or techniques of 'social engineering' where victims were persuaded to part with the details at the request of an ostensibly legitimate source. At its peak, *Dark Market* was the world's pre-eminent English language 'carding' site, with over 2500 members from a number of countries around the world, including the United Kingdom, Canada, the United States, Russia, Turkey, Germany and France.[45]

Operation Olympic Games is reportedly a collaboration between the US National Security Agency and its Israeli counterpart, Unit 8200, intended to disrupt the Iranian nuclear

enrichment program. It allegedly involved the clandestine insertion of an extremely complex and sophisticated set of software into communications and control systems at the Natanz nuclear facility. The software reportedly includes a capacity to monitor communications and processing activity, as well as the ability to corrupt control systems at the facility. The operation succeeded in delaying the progress of uranium enrichment through remote controlled destruction of a number of centrifuges used in the process. The secrecy surrounding the operation was compromised in part when the malicious software escaped because of a programming error. Neither the United States nor the Israeli governments have yet to acknowledge the existence of the operation.[46]

Ghost Net was the name given by a group of Canadian researchers in 2010 to a cyber-espionage operation apparently operating from commercial internet accounts in China. The hackers compromised government computers in over 100 countries on several continents; they also targeted emails from the server of the Dalai Lama. The Chinese Government denied involvement, and there was no conclusive evidence to the contrary. There is, however, some evidence of government complicity. Chinese officials have confronted expatriate dissidents returning to China with transcripts of internet chats in which they were involved during their absence.[47] Whether the activity in question was the work of patriotic hackers acting unilaterally, or skilled individuals with guidance from state authorities who were otherwise acting at arm's-length, remains unclear. Canadian investigators claim to have found evidence of links to two individuals in the underground hacking community of the PRC.[48]

PLA Unit 61398

In February 2013, the information security company Mandiant reported that a large scale program of industrial espionage had been undertaken in 2006 by Unit 61398 of the People's Liberation Army. Based in Shanghai, this organization is alleged to have acquired a massive volume of data from a wide variety of industries in English speaking countries. Information alleged to have been taken includes technical specifications, negotiation strategies, pricing documents and other proprietary data. One of the alleged targets, a major US beverage manufacturer, was planning in 2009 what was to have been the largest foreign purchase of a Chinese company to date. It was reported that an apparently innocuous email to an executive of the US company contained a link, which when opened, allowed the attackers access to the company network. Sensitive information on pending negotiations was reportedly accessed by

Chinese intruders on a regular basis; the purchase did not eventuate. It is unclear whether the unit is staffed exclusively by military personnel or includes civilian contractors.[49]

Conclusions

The above examples of organized cyber criminality enable one to conclude that not all organizations acting illegally in cyberspace may be regarded as threats to national or international security. Some activity is unquestionably annoying, offensive in the extreme, and/or harmful. There are online activities which, if writ large, might conceivably weaken the integrity and economy of states and thus come to be regarded as security threats. Online paedophilia, no matter how heinous or distasteful one might regard it, does not occur on a scale at which a nation's economy or social fabric is damaged. Nor is it likely ever to do so. The software and entertainment industries in the United States have sought to make the case that information piracy costs the domestic economy millions of dollars in lost profits, and has a chilling effect on entrepreneurialism and creativity world-wide. However, the US economy is sufficiently diverse that its future strength will depend on other factors. Indeed, one could argue that piracy allows citizens of less developed countries to benefit from access to products that they would otherwise be unable to afford. By contrast, major, persistent industrial or political espionage on a wider scale may well threaten the security of the target state.[50] Industrial espionage can weaken the international competitiveness of a company or of an industry sector. When the information in question relates to weapons systems, the security implications are obvious.

Theft of credit card and banking details, were it to occur on a larger scale, would certainly impede commercial activity, with corresponding harm to a state's economy. For the time being, however, online fraud appears manageable. Technologies of information security continue to be refined, and tech savvy members of the public, at least in developing countries, are able to protect themselves. On line banking and e-commerce continue to thrive.

In less developed countries, however, where users are just entering the digital age, lack of awareness of cybersecurity may enhance the vulnerability of individuals and of organizations in both the public and private sectors. To the extent that the threat of cybercrime impedes the development of electronic commerce, it could contribute to the weakening of a nation's security.

As far as organizations are concerned, it appears that the greatest threats to national security are posed by states themselves, either singlehandedly or in collaboration with skilled amateurs or sophisticated cybercriminals. The activity reported to have led to the destruction of Iranian centrifuges would certainly be defined by authorities of that country (or those of any other nation on the receiving end of a similar attack) as a security threat. Nations on the receiving end of similar attacks might be inclined to regard them as acts of cyber-war.[51]

The activities of *Anonymous*, such as eavesdropping on a conference call between law enforcement agents and attempts to shut down the website of the Central Intelligence Agency, have certainly been found annoying by authorities in the United States. On the scale at which they were conducted, such activities were certainly embarrassing, but would not constitute harm to national security. Such activity, if undertaken persistently or on a larger scale, might send a message of state nonchalance at best, and incompetence at worst, and thereby invite imitation from many quarters. The potential for significant harm is therefore real. The threshold of objective threat would appear to be a function of the scope and intensity of criminal activity on the one hand, and the resilience of the state and its infrastructure on the other.

The disclosures of Wikileaks may have impeded US diplomats from obtaining candid comments from local informants around the world. Some of these disclosures appear to have enhanced the vulnerability of weak regimes, and to that end, organized cybercrime was certainly a threat to *their* security. Whether this will enhance or detract from the security of the United States remains to be seen.

If organized cybercrime were to occur on a greater scale, it could lead to a weakening of trust in major public or private institutions. The fundamental question for our purposes is at what point does the nature and scale of online criminal activity (organized or otherwise) begin to constitute a security threat. National security is not a binary variable. The question is not "are you, or are you not, secure?" but rather "might a specific circumstance contribute to an enhancement or diminution of security?"

Many of those criminals operating in cyberspace, alone or in organizations, were competent technicians before turning to crime. What is interesting is the relatively minor role that conventional "terrestrial" organized criminal groups have thus far played in cybercrime.[52] Their main use of internet technology appears to have been incidental, as media of communications and of record keeping. One has seen examples of conventional criminal

organizations engaging IT specialists for specific tasks. This pattern of engagement is not unlike that of large scale drug offenders who contract with chemists to assist in the refinement of heroin or the manufacture of synthetic drugs. In one case, associates of the New York-based Bonnano crime family, were charged with various offences including the illegal manufacture of fraudulent checks, and fraud in connection with access devices. The group included one individual with a background in computing who accessed data bases with a view towards identifying potential extortion victims. He also used his computing skills in the production of counterfeit checks.[53] Meanwhile, digital technology with direct criminal application is becoming more sophisticated and more widely accessible. The potential for malicious software kits or "exploits, " to be used by, or sold commercially by, criminal organizations, is already significant and is destined to increase.[54] There seems little doubt that that conventional organized criminals who have grown up in the digital age will embrace the technology as a matter of routine, if they have not already done so, for purposes both mundane and illicit.

Given the current pervasiveness of digital technology, its accessibility to criminal organizations, and its utility for a variety of criminal ends, there seems little doubt that the potential threat to national and international security will persist. The challenge, as is the case with purely terrestrial matters, is to distinguish the real from the illusory.

Acknowledgements:

The author is grateful to Dr Grant Wardlaw and two anonymous reviewers for comments on an earlier version of this paper.

[1] The term securitization was coined by Wæver to refer to this conceptual expansion. Wæver, Ole (1995) 'Securitization and Desecuritization', in Ronnie D. Lipschutz (ed.) *On Security*, pp. 46–86. New York: Columbia University Press.

[2] The first academic references to human security date back nearly 50 years. See Blatz, William E. (1966) *Human security; some reflections*. University of Toronto Press, Toronto.

[3] Sun Tzu, *The Art of War* (Samuel B Griffith Tr) Oxford University Press, London, 1971, pp 113-114.

[4] "US Initiatives against International Organized Crime" remarks of William J Clinton, President of the United States, at the 50th Anniversary Assembly of the United Nations, New York City, October 22, 1995.

[5] Weiner, Tim (2012) Enemies: A History of the FBI. Random House, New York, pp197-201.

[6] *New York Times Co. v. United States* (403 U.S. 713)

[7] http://www.house.gov/apps/list/hearing/ny03_king/kingsupportsprosecutionofwikileaks.html (accessed May 20, 2013)

[8]Weiner, Tim (2007) Legacy of Ashes: A History of the CIA. Doubleday, New York, pp 320-330.

[9] Buzan, Barry (2004) The United States and the Great Powers: World Politics in the Twenty-First Century. Polity Press, Cambridge UK. p 172.

[10] http://www.organized-crime.de/OCDEF1.htm (accessed May 20, 2013).

[11] Cressey, Donald R (1972) Criminal Organization: Its elementary forms. Heinemann Educational Books, London

[12] Halstead, Boronia. 1998. "The Use of Models in the Analysis of Organized Crime and Development of Policy." *Transnational Organized Crime* 4(1): 1–24.

[13] Williams, Phil. 2001. "Transnational Criminal Networks." In *Networks and Netwars*, edited by John Arquilla and David Ronfeldt. Santa Monica: Rand Corporation; Morselli, Carlo (2008) Inside Criminal Networks. Springer, New York.

[14] Stohl, M. (1998) "Demystifying Terrorism: The Myths and Realities of Contemporary Terrorism. " In M. Stohl (ed) The Politics of Terrorism. Marcel Dekker, New York, p 3.

[15] Grabosky, Peter and Michael Stohl (2010) Crime and Terrorism. Sage Publications, London. Makarenko, Tamara (2004) "The Crime Terror Continuum" Global Crime, 6, 1, 129-145. Peter Grabosky and Michael Stohl (2003) "Cyberterrorism" Reform, 82, 8-13. Mincheva, L. and Gurr, T. (2013) *Crime-Terror Alliances and the State: Ethnonationalist and Islamist Challenges to Regional Security,* Routledge: Abingdon.

[16] Perl, Raphael (2007) Drug Trafficking and North Korea: Issues for U.S. Policy Congressional Research Service, Washington D.C. http://www.fas.org/sgp/crs/row/RL32167.pdf (accessed May 20, 2013).

[17] Grabosky, Peter (1995) 'Using Non-governmental Resources to Foster Regulatory Compliance', Governance: An International Journal of Policy and Administration, 8, 4, 527-50.

[18] Martin, Brian G (1996) The Shanghai Green Gang: Politics and Organized Crime 1919-1937 Univerrsity of California Press, Berkeley; Wakeman, Frederick Jr (1995) Policing Shanghai, 1927-1937 University of California Press, Berkeley

[19] Weiner, Tim (2007) Legacy of Ashes: The history of the CIA. Doubleday, New York.

[20] Standing, Andre (2003) The Social Contradictions of organized crime on the Cape Flats. Institute for Security Studies Occasional paper 74. Institute for Security Studies, Pretoria.

[21] The nature of this content varies widely across jurisdictions; it may include neo-Nazi propaganda , advocacy of Tibetan independence, or child pornography, among much else.

[22] The individual in question hacked into a telephone network which resulted in incapacitation of the air trafficcontrol system. See United States Department of Justice (1998) Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport—First Federal Charges Brought Against a Juvenile for Computer Crime. Press Release March 18 http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm (accessed 5 April 2003); http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/01/18/mafiaboy010118; US Securities and Exchange Commission (2000) In the Matter of Jonathan G. Lebed http://www.sec.gov/litigation/admin/33-7891.htm (accessed May 20, 2013).

[23] SSC Silva,S., Silva, R., Pinto, R., and Salles, R. (2013) Botnets: A Survey. Computer Networks, 57, 2, (4 February), 378–403.

[24] Chang, L. Y. C. (2012). *Cybercrime in the Greater China Region: Regulatory Response and Crime Prevention across the Taiwan Strait*. Cheltenham: Edward Elgar.

[25] See the discussion of Operation Olympics Games, below, and Sanger, David (2012) Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. Crown Publishers, New York.

[26] Sipress, A. (2004) "An Indonesian's prison memoir takes Holy War into cyberspace": In Sign of New Threat, Militant Offers Tips on Credit Card Fraud, *Washington Post*, December 14, A19 http://msl1.mit.edu/furdlog/docs/washpost/2004-12-14_washpost_jihadis_online.pdf (accessed May 20, 2013).

[27] U.S. National Intellectual Property Rights Coordination Center (2011). Intellectual Property Rights Violations: A Report on Threats to United States Interests at Home and Abroad http:// www.iprcenter.gov/reports (accessed May 21, 2013; http://globalstudy.bsa.org/2011/ (accessed 21 May 2013) ;http://blog.mpaa.org/BlogOS/post/2011/09/08/Correcting-the-Record-on-the-Financial-Impact-of-Content-Theft.aspx . But see Anderson, R., Barton, C. Boehme, R. Clayton, R., van Eeten, M., Michael Levi, M., Moore, T., and Savage, S. (2012) Measuring the Cost of Cybercrime. 11th Workshop on the Economics of Information Security, Berlin, Germany, June 26. http://lyle.smu.edu/~tylerm/weis12pres.pdf (accessed May 21, 2013).

[28] Glenny, Misha (2011) Dark Market. Knopf, New York.

[29] Stoll, Clifford (1989) The Cuckoo's Egg. Doubleday, New York.

[30] http://wikileaks.org/

[31] Schneider, Jacqueline L. 2003. "Hiding In Plain Sight: An Exploration of the Activities of a Drugs Newsgroup." Howard Journal of Criminal Justice 42(4): 372–389.

[32] Moghadam, Assaf (2009) The Globalization of Martyrdom:Al Qaeda, Salafi Jihad, and the Diffusion of Suicide Attacks. The Johns Hopkins University Press, Baltimore, p 146.

[33] Mayer, Jane (2009) The Dark Side: The Inside Story of how the War on Terror Turned into a War on American Ideals. Anchor Books, New York; Prost, Dana and Arkin, William M. (2011) Top Secret America: The Rise of the New American National Security State. Little Brown, New York.

[34] Edwards, O. (1995) Hackers from Hell. Forbes, 9 October, 182.

[35] See Note 18 supra and accompanying text; Grabosky, Peter (2007) Electronic Crime. Upper Saddle River, NJ. Pearson Prentice Hall

[36] Grabosky, Peter and Smith, Russell G (1998) Crime in the Digital Age Controlling Telecommunications and Cyberspace Illegalities. Federation Press, Sydney and Transaction Publishers, New Brunswick, NJ.

[37] Bumiller, Elizabeth and Shanker, Thom (2012) Panetta Warns of Dire Threat of Cyberattack on U.S. The New York Times October 11 http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=1 (accessed May 20, 2013).

[38] Brodkin, Jon (2007) Government-sponsored cyberattacks on the rise, McAfee says: The future holds more cyber-espionage, attacks against government systems Network World November 29, 2007 http://www.networkworld.com/news/2007/112907-government-cyberattacks.html (accessed May 20, 2013).

[39] The information in question was allegedly provided to Wikileaks on a CD-ROM, and thereafter disseminated on theInternet. Shane, Scott and Lehren, Andrew W. (2010) "Cables Obtained by WikiLeaks Shine Light Into Secret Diplomatic Channels" The New York Times, 28 November. http://www.nytimes.com/2010/11/29/world/29cables.html?hp (accessed May 20, 2013).

[40] Russell, Gabrielle (2008) "Pedophiles in Wonderland: Censoring the Sinful in Cyberspace." Journal of Criminal Law and Criminology, 98, 4, 1467-1500; Graham, William R, Jr (2000) Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland.' Law Review of Michigan State University- Detroit College of Law, 2000, 457-484.

[41] Denning, Dorothy (2001) "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy." In John Arquilla, David F. Ronfeldt (eds) Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation, Santa Monica; Olson, Parmy (2012) We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Little, Brown, New York;

[40] Coleman, Gabriella (2011) Anonymous: From the Lulz to Collective Action.The New Everyday, 6 April. http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action (accessed May 20, 2013);
Olson, Parmy (2012) We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Little, Brown, New York.

[43] http://www.justice.gov/criminal/cybercrime/press-releases/2001/warezoperations.htm (accessed May 20, 2013); Lee, Jennifer (2002) Pirates on the Web, Spoils on the Street. New York Times, July 11, 2002. http://www.nytimes.com/2002/07/11/technology/pirates-on-the-web-spoils-on-the-street.html?pagewanted=all&src=pm (accessed May 20, 2013); McIllwain, Jeffrey (2005) Intellectual Property Theft and Organized Crime: The Case of Film Piracy. Trends in Organized Crime, 8, 4, 15-39; Urbas, Gregor (2006) Cross-national Investigation and Prosecution of Intellectual Property Crimes: The Example of 'Operation Buccaneer' Crime, Law and Social Change, 46, 207-221; US Department of Justice (2002) Warez Leader Sentenced to 46 Months (May 17, 2002) http://www.justice.gov/criminal/cybercrime/press-releases/2002/sankusSent.htm (accessed May 20, 2013)

[44] http://www.fbi.gov/newyork/press-releases/2012/another-cyber-fraud-defendant-charged-in-operation-aching-mules-sentenced-in-manhattan-federal-court (accessed May 20, 2013); http://www.justice.gov/usao/nys/pressreleases/September11/garifulinnikolaypleapr.pdf (accessed May 20, 2013);http://www.fbi.gov/newyork/press-releases/2010/nyfo093010.htm (accessed May 20, 2013); http://www.justice.gov/usao/nys/pressreleases/September10/operationachingmulespr%20FINAL.pdf (accessed May 20, 2013).

[45] Glenny, Misha (2011) Dark Market. Knopf, New York.

[46] Sanger, Confront and Conceal. The full consequences of the operation are uncertain, as neither the victims nor the perpetrators are inclined to discuss it. With knowledge of its very existence now widespread, others may follow the example of perpetrators and engage in cyber attacks for their own purposes. The

ultimate consequences of this are unpredictable. Recent electronic attacks against U.S. financial institutions and Saudi oil facilities may represent two examples. Perlroth, N. (2012) "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back" New York Times, October 23 http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all (accessed May 20, 2013); Perlroth N. and Hardy, Q. (2013) "Bank Hacking Was the Work of Iranians, Officials Say" *New York Times*, January 8 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html (accessed May 20, 2013).

[47] Information Warfare Monitor (2009) Tracking GhostNet: Investigating a Cyber Espionage Network. March 29, P.28 http://www.infowar-monitor.net/ghostnet (accessed May 20, 2013).

[48] http://www.nartv.org/mirror/shadows-in-the-cloud.pdf; Markoff, John and Barboza, David (2010) Researchers Trace Data Theft to Intruders in China New York Times, 5 April http://www.nytimes.com/2010/04/06/science/06cyber.html?pagewanted=all (accessed May 20, 2013).

[49] http://intelreport.mandiant.com/ (accessed May 20, 2013): Sanger, D., Barboza, D. and Perlroth, N (2013) "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *New York Times* February 18. http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all (accessed May 20, 2013).

[50] Office of the National Counterintelligence Executive (2011) Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011. http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed May 20, 2013)

[51] Turns, David (2012) Cyber Warfare and the Notion of Direct Participation in Hostilities. Journal of Conflict Security Law, 17, 2, 279-297.

[52] For a different view, see Maguire, M (2012) Organized Crime in the Digital Age. John Grieve Centre for Policing and Security, London Metropolitan University.

[53] Indictment, US v Fiore et al (2009) http://www.justice.gov/usao/fls/PressReleases/Attachments/090521-02.Indictment.pdf (accessed May 20, 2013).

[54] Alazab, M., Venkatraman, S., Watters, P., Alazab, M., and Alazab, A. (2012) **"**Cybercrime: The Case of Obfuscated Malware**"** *Global Security, Safety and Sustainability & e-DemocracyLecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, 99, 204-211.